System

The following settings are always required for proper operation of TightGate-Pro:

Menu item	Description
Hostname	Name of TightGate-Pro, can be selected according to the target environment. For cluster systems, the name always ends with the consecutive number in the cluster.
Domain*	Network domain in which TightGate-Pro is operated.
DNS name in Cert*	DNS name of TightGate-Pro that can be resolved by the client and is entered in the user certificate for authentication at TightGate-Pro. For cluster systems, the domain name of the TightGate-Pro cluster must be entered here.
Ctrl-Alt-Del action*	The key combination can be used to restart the system or to shut it down correctly.
Web interface password*	If a password is set here, it must be entered to call up the status page of status page of TightGate-Pro must be entered on the client side under http://localhost on the client side. Username ist always **status**

Language settings

TightGate-Pro supports multilingualism in administration and for the user interface. The language settings are configured via the ***Language settings*** menu.

Hint

Multilingualism when entering country-specific special characters is realised in TightGate-Pro with the "IBus" (Intelligent Input Bus) framework. You can find instructions on how to use Ibus here.

Admin menus
Selection of the language to be used for the administration of TightGate-Pro. This setting affects all administration menus equally and only becomes effective after a new login. The languages German and English are available.

Users (VNC)
Selection of the default language for all TightGate users. For users who are already logged in, the setting only takes effect the next time they log in to TightGate-Pro. A user language that differs from this global system default can be set as administrator ***maint*** for each user individually. The prerequisite for this is that the language is installed on each TightGate-Pro node. If the desired language is not yet available in the menu, it must be set to (as described here) must be installed on each TightGate-Pro node.

Hint

The setting takes effect immediately for all users after leaving the menu and overwrites the language set as ***maint*** user language.

Renew CA certificate

The CA certificate is the root certificate of TightGate-Pro and is required for all types of user authentication. The CA certificate is valid for 20 years, but the period of validity can be set by the user. The current validity of the CA certificate is displayed behind the menu item **Renew CA certificate**. If the validity is less than 60 days, you should carry out a renewal and customise the users of TightGate-Pro for the new CA.

Warning

In any case, make sure that the CA certificate is valid and has not expired, otherwise users will no longer be able to log on to TightGate-Pro.

How to renew the CA certificate:

- Log in as user ***config*** and then select the menu item **System > Renew CA certificate**.
- A security prompt appears asking whether the CA certificate should really be renewed. After confirming this, an input field appears in which you can change the validity period of the CA certificate. The default value of 7301 days corresponds to 20 years. The maximum value is 9999 days (~27 years). After confirming this entry, the CA certificate is renewed.
- An **Save** and **Apply** is required so that the CA certificate is generated and, if required, distributed in the cluster.

Hint

Existing user certificates will remain valid until the original CA expires. However, the old certificates will be removed from the ***config***-transfer directory and will no longer be displayed under ***maint***. New certificates must be generated and exported for the new CA via the menu option **User management > Create SSL Keys** for all Users.

After the CA certificate has been renewed, the new validity is displayed behind the menu item Renew CA certificate. To send the new CA to the clients, the certificate files for the certificate enrolment must be must be re-exported and distributed. If user authentication is carried out via Active Directory, the CA certificate must be provided centrally on the Windows computers centrally.

Licence management

In order to use TightGate-Pro, a valid licence must be purchased and properly stored in the system. In case of doubt, the technical customer service team at m-privacy GmbH can provide support and advice on all questions relating to the licensing of TightGate-Pro.

Importing a license

The license file sent by m-privacy GmbH must be copied to the administrator's transfer directory ***config*** transfer directory:

```
/home/config/transfer
```

This can be done by the administrator ***config*** or the user ***transfer*** via the TightGate-Schleuse program.

The actual import of the license is carried out by the administrator ***config***. When calling up the menu item **System > Import License**, all license files stored in the directory specified above are displayed. Select the desired license file and confirm the import with **OK** to confirm the import. The license becomes effective after the option **Apply** option in the main menu.

For TightGate-Pro cluster systems, the license file only needs to be installed on one computer in the cluster (node). The license is automatically distributed to the other nodes in the cluster during operation.

Achtung

If the TightGate-Pro license cannot be imported, one possible cause is an incorrectly registered virus scanner. Please check the virus scanner as described here.

Checking the license capacity

It is possible to read out the number of available licenses. The administrator ***config*** can view the license file via the menu item **System > Show License**.

It is also possible to open a browser on TightGate-Pro and call up the status page http://localhost/. Depending on the default settings, the entry of access data (for the user **status**) is required. The password for the user **status** user is assigned when the system is installed. The password is changed as administrator ***config*** via the menu item **System > Web interface password**. If no password is assigned, the status page can be viewed by any TightGate user via the browser.